

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-311674

(43)Date of publication of application : 28.11.1995

---

(51)Int.Cl.	G06F	7/58
	G09C	1/00
	H04K	1/00
	H04L	9/00
	H04L	9/10
	H04L	9/12

---

(21)Application number : 06-102988

(71)Applicant : NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 17.05.1994

(72)Inventor : MORITA HIKARI  
ABE MASAYUKI  
AOYAMA MASAO

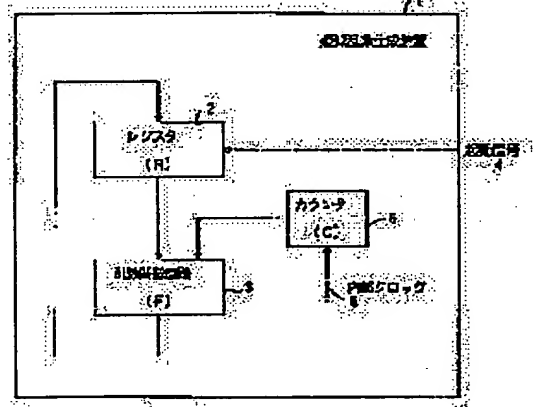
---

## (54) PSEUDO-RANDOM NUMBER GENERATION DEVICE

### (57)Abstract:

**PURPOSE:** To provide the pseudo-random number generation device which generates random numbers enabling safe key distribution, opposite-user confirmation, etc., while keeping the random numbers safe even under various conditions.

**CONSTITUTION:** The pseudo-random number generation device 1 is equipped with a counter 5 which counts a value C, a register 2 wherein a value R is stored, and a random number function circuit 3 which inputs the value C of the counter 5 and the value R of the register 2 and outputs a random number function  $F(R,C)$ , and updates the value R in the register 2 with the random number function  $F(R,C)$  outputted from the random number function circuit 3 in response to a start signal.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-311674

(43) 公開日 平成7年(1995)11月28日

(51) Int.Cl. <sup>a</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 7/58	B			
G 0 9 C 1/00		9364-5L		
H 0 4 K 1/00	Z			
H 0 4 L 9/00				

H 0 4 L 9/ 00

Z

審査請求 未請求 請求項の数3 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願平6-102988

(22) 出願日 平成6年(1994)5月17日

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 森田 光

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 阿部 正幸

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 青山 政夫

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74) 代理人 弁理士 伊東 忠彦

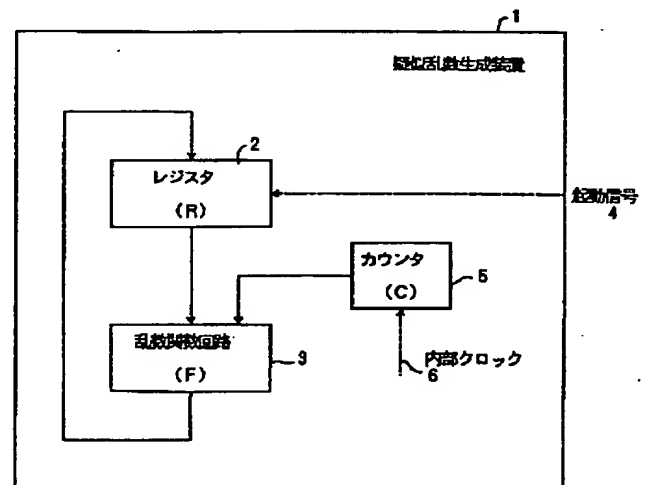
(54) 【発明の名称】 疑似乱数生成装置

(57) 【要約】

【目的】 本発明の目的は、種々の条件下でも乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる乱数を生成する疑似乱数生成装置を提供することである。

【構成】 本発明の疑似乱数生成装置1は、値Cをカウントするカウンタ5と、値Rを蓄積するレジスタ2と、カウンタ5の値C及びレジスタ2の値Rが入力され、乱数関数F(R, C)を出力する乱数関数回路3とを具備し、起動信号を契機として乱数関数回路3から出力される乱数関数F(R, C)によりレジスタ2の値Rを更新する。

本発明の一実施例の疑似乱数生成装置の構成図



## 【特許請求の範囲】

【請求項 1】 値 C をカウントするカウンタと、  
値 R を蓄積するレジスタと、  
該カウンタの値 C 及び該レジスタの値 R が入力され、乱  
数関数  $F(R, C)$  を出力する乱数関数回路とを具備  
し、  
起動信号を契機として該乱数生成部から出力される該乱  
数関数  $F(R, C)$  により該レジスタの値 R を更新する  
ことを特徴とする疑似乱数生成装置。

【請求項 2】 前記カウンタは、  
内部クロックが前記起動信号と独立に与えられ、該内部  
クロックに基づいて逐次的に前記カウンタの値 C を更新  
する請求項 1 記載の疑似乱数生成装置。

【請求項 3】 前記内部クロックは、外部からの観測不  
能とし、  
前記カウンタは、前記内部クロックに基づいて逐次的に  
カウンタの値 C を更新することにより、外部から与えら  
れる前記起動信号が前記カウンタの値 C を更新する周期  
と無関係に与えられる請求項 1 記載の疑似乱数生成装  
置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、疑似乱数生成装置に係  
り、特に、暗号通信、鍵配送、相手認証等で必要となる  
乱数を生成する疑似乱数生成装置に関する。

【0002】近年、2 者間で通信において、相互に安全  
な鍵配送、相手認証等を行う端末や装置等のシステム中  
に内蔵される疑似乱数生成装置は、従来から求められて  
いる処理の再現性、計算機の資源のコンパクト化に加  
え、外部からの乱数値の類推が不可能な安全性の高さが  
求められている。

## 【0003】

【従来の技術】鍵配送、相手認証等では、外部から推測  
できない安全な乱数が求められている。一般の乱数につ  
いては、KNUTH 著：『準数値算法／乱数』（サイエ  
ンス社刊、p 3）で紹介されているように、処理の正当  
性の再現性、計算機資源のコンパクト化（メモリ削減）  
の要請から、関数を使った乱数生成法が利用される。

【0004】例えば、関数  $F$  が初期値  $R_{(0)}$  より順番に  
乱数列  $R_{(1)}$ 、 $R_{(2)}$ 、 $R_{(3)}$ 、…を生成する。個々  
に、乱数列の ( ) 内の添字は、乱数列  $R$  の順番を示すも  
ので、 $R_{(i+1)} = F(R_{(i)})$ （但し、 $i \geq 0$ 、整数）  
なる関係があるとする。初期値が決まると全ての乱数列  
が決まるので、理想的な乱数列とは区別し、乱数列  $R_{(0)}$   
、 $R_{(1)}$ 、 $R_{(2)}$ 、 $R_{(3)}$ 、…を疑似乱数列と呼び、  
 $F$  は疑似乱数関数と呼ぶ。

【0005】上記の乱数生成法における課題は、 $|X|$   
が  $X$  を取りうる全ての値の個数とすると、 $R_{(i+1)} = F$   
( $R_{(i)}$ ) で定義される疑似乱数列の周期が上限の  $|R|$   
に近いかということと、本来の乱数生成の要請

である、値の分布が一樣にばらつくかどうかということ  
である。

【0006】図 4 は、従来の疑似乱数生成装置のブロッ  
ク図である。同図に示す疑似乱数生成装置 1 は、レジス  
タ 2 及び乱数関数回路 3 より構成される。レジスタ 2  
は、値 R が設定され、外部から起動信号 4 が入力される  
毎に、乱数生成回路 3 から出力される値 F によりレジス  
タ 2 の蓄積値 R を更新し、レジスタ 2 は、その値 F

(R) を保持する。ここで、レジスタ 2 の値 R の初期設  
定をしなくてもよいが、多くの場合、電源投入時に値 R  
を蓄積するレジスタ 2 または、RAM の物理的な特性に  
より特定値に偏る。また、常に起動信号 4 が発生する状  
態にし、値 R の更新回数を増大させる方法もある。

【0007】図 5 は、従来の疑似乱数生成装置の動作を  
示すフローチャートである。疑似乱数生成装置 1 は、外  
部から起動信号 4 が入力されるまで、待機し、起動信号  
4 が入力されると（ステップ 1）、レジスタの疑似乱数  
R が  $F(R)$  で更新される（ステップ 2）。

【0008】また、鍵配送で代表的な DH 法（池野、小  
山著：『現代暗号理論』、電子情報通信学会間、pp.  
175-177）を A と B の 2 者間で行う場合、A は、  
 $R_A$ 、B は、 $R_B$  なる乱数を生成し、A から  $\alpha \wedge R_A \bmod P$   
、B から  $\alpha \wedge R_B \bmod P$ （なお、 $X \wedge Y$  は、 $X$  を  $Y$   
乗することを表す。 $X \bmod Y$  は、 $X$  を  $Y$  で除した余り）  
を相手に送信する。この結果、両者で共通鍵  $K = \alpha \wedge$   
( $R_A R_B$ )  $\bmod P$  を共有する。このとき、悪意の第 3  
者が、 $\alpha \wedge R_A \bmod P$ 、 $\alpha \wedge R_B \bmod P$  なる通信デー  
タを入手し、システムパラメータの  $\alpha$ 、 $P$  を知っても、共  
有鍵  $K$  を生成することはできない。この方法は、A また  
は、B において、システムに内蔵される疑似乱数装置を  
用いる。

## 【0009】

【発明が解決しようとする課題】しかしながら、図 4 に  
示す従来の疑似乱数生成装置は、レジスタに蓄積される  
値 R の初期設定を行わないと、電源投入時に R を蓄積す  
るレジスタまたは、RAM の物理的な特性により、特定  
の値に偏るという問題がある。また、常に、起動信号が  
入力される状態にし、レジスタの値 R の更新回数を増大  
させる方法は、消費電力削減の点からは好ましくない。

【0010】さらに、DH 法は、第 3 者が乱数  $R_A$  を予  
測できた場合には、A と同様に、 $\alpha \wedge R_B \bmod P$  から共  
有鍵  $K$  を生成できるので、安全な鍵配送が行うことがで  
きない。従って、乱数が外部から推測できないことが要  
請される。

【0011】一方、一般にシステム中に内蔵される疑似  
乱数生成装置は、生産上の理由から以下の事象が起きや  
すい。

(1) 大量生産における生産・検査工程の簡単化のた  
め、同じ構造の装置を生産する。

(2) 装置の電源を切ると、物理的特性から決まる特定

の値に初期化される。

(3) 複数業者へ装置使用の技術開示をすることがあり、構造の秘匿性は確保できない。

【0012】この結果、例え、疑似乱数列  $R_{(0)}$ 、 $R_{(1)}$ 、 $R_{(2)}$ 、 $R_{(3)}$ 、…が長い周期をもつように疑似乱数関数  $F$  が設計されていたとしても、悪意の第3者が装置の電源を切る、または、装置の動作回数を観測することにより、予測する乱数の探索空間を狭めることができ、従来の方法のままでは十分な対策とはなり得ないという問題がある。

【0013】また、悪意の第3者が正規の通信により、 $A$ のある時点における乱数  $R$ を知り、その後の  $A$ による乱数の探索空間を狭めることが可能である。例えば、 $RSA$ 暗号により、 $A$ が  $B$ の正当性を確かめる場合を考える。つまり、 $A$ が乱数  $R$ を  $B$ に送り、 $B$ は、 $B$ の秘密鍵  $(d, N)$ で、

$$C \leftarrow R \wedge d \bmod N$$

を実行し、 $C$ を  $A$ に送信し、 $B$ の公開鍵  $(e, N)$ を用いて、 $A$ が  $C \wedge e \bmod N$ を実行し、結果が乱数  $R$ に一致するかを確かめる手順を考える。この手順が安全に目的を果せたとしても、直前の  $R$ の値から続く上記の  $DH$ 法における乱数が予測できる。

【0014】これに対する有効な手段は、乱数関数  $F$ が乱数  $R$ 以外の第2パラメータ  $K$ によって変化する関数とし、 $R \leftarrow F(R, K)$ で疑似乱数列を生成することである。多くの場合、乱数関数  $F$ は、暗号関数または、暗号関数を複数組み合わせで構成され、 $K$ は、暗号関数の暗号鍵となることが多い。しかしながら、上記のように、乱数の一時の値が外部に既知となると、前後の乱数  $R_{(i)}$ 、 $R_{(i+1)}$ を観測し、 $R_{(i+1)} = F(R_{(i)}, K)$ となる関数  $F$ の入出力から、暗号関数  $F$ の既知平文攻撃を構成でき、採用される暗号関数の安全性に全体の安全性が左右され、完全な解決策を与えるに至らない。

【0015】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、装置が全く同じ構造、初期化され同じ状態になる、装置使用の技術開示がなされているような条件下でも乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる乱数を生成する疑似乱数生成装置を提供することを目的とする。

#### 【0016】

【課題を解決するための手段】本発明の疑似乱数生成装置は、値  $C$ をカウントするカウンタと、値  $R$ を蓄積するレジスタと、カウンタの値  $C$ 及びレジスタの値  $R$ が入力され、乱数関数  $F(R, C)$ を出力する乱数生成回路とを具備し、起動信号を契機として乱数生成回路から出力される乱数関数  $F(R, C)$ によりレジスタの値  $R$ を更新する。

【0017】また、本発明の上記のカウンタは、内部クロックが起動信号と独立に与えられ、内部クロックに基づいて逐次的にカウンタの値  $C$ を更新する。

【0018】また、本発明の上記の内部クロックは、外部からの観測不能とし、カウンタは、内部クロックに基づいて逐次的にカウンタの値  $C$ を更新することにより、外部から与えられる起動信号がカウンタの値  $C$ を更新する周期と無関係に与えられる。

【0019】即ち、本発明の疑似乱数生成装置は、内部クロックに基づいて繰り返し動作するカウンタを自走させ、クロックとは非同期な起動信号または、コマンドによる起動信号を契機に、カウンタ値  $C$ を特定して、乱数関数回路から出力される乱数関数  $F$ により、レジスタに蓄積される乱数  $R$ を  $R \leftarrow F(R, C)$ の手続により更新する。

#### 【0020】

【作用】本発明は、カウンタを起動する内部クロックとは非同期なタイミングで入力される起動信号を利用することにより、外部から観測できないカウンタの値  $C$ を用いて、次の乱数  $R$ を生成するため、前の乱数の値  $R$ に加え、カウンタの値を特定しない限り、悪意の第3者は、その後の乱数は予測することができない。

【0021】従って、装置使用、初期値等の内部情報が公開し、外部から乱数更新回数を観測しても、正確にカウンタの動きを外部から予測できない。カウンタの値を特定するには、装置内部を観測するまでの工作が必要であり、安全である。

#### 【0022】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【0023】図1は、本発明の一実施例の疑似乱数生成装置の構成を示す。同図において、図4と同一構成部分には、同一符号を付与する。疑似乱数生成装置1は、乱数  $R$ を蓄積するレジスタ2、乱数関数回路3、起動信号4に加え、内部クロック6に同期して動くカウンタ5が具備される。

【0024】〔第1の実施例〕上記の構成により第1の実施例を説明する。

【0025】第1の実施例は、カウンタ5を内部クロック6に基づいて繰り返し動作させ、内部クロック6とは非同期な外部信号を起動信号4として、カウンタ5の値を特定して乱数関数  $F$ によりレジスタ2の値  $R$ を更新するものである。

【0026】図2は、本発明の第1の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【0027】装置の動作が開始されると、カウンタ5と乱数関数回路3の動作は、同時並行的に行われる。つまり、カウンタ5は、内部クロック6に同期してカウントアップして  $C \leftarrow G(C)$ を繰り返す。ここで、関数  $G$ は、 $C \leftarrow C + 1 \bmod T$  ( $T$ はカウンタの周期)でもよいし、カウンタ5の値  $C$ を2進数で一様ランダムな値をとる非線形フィードバックレジスタ構成でもよく、取り得る数値の変動幅（または、2進数表現時のハミング距

離) がランダムに変動してもよい (ステップ 101)。

【0028】外部からの起動信号 4 が入力されると (ステップ 102)、乱数生成回路 3 は、レジスタ 2 の値 R とその時点のカウント 5 の値 C の値から乱数関数 F

(R, C) を生成し、この乱数関数でレジスタ 2 の値 R を更新する。

【0029】起動信号 4 が内部クロック 6 と独立に発生することが重要であり、カウンタ 5 の値 C が取り得る値の個数を T とした場合、予め起動信号 4 を L 回起動しておく、T × L 通りの探索空間に広げることができる。

【0030】従って、初期状態を類推できても、実際に使う疑似乱数の前に予め起動信号を L 回起動しておく、T × L 通りの探索空間に広げることができる。

【0031】また、上記の相手確認の場合のように、疑似乱数が直接外部に漏れることがあっても起動信号 4 を L 回起動してから疑似乱数を使用することにより、T × L 通りの探索空間に広げることができる。

【0032】[第 2 の実施例] 次に、図 1 の構成に基づいて、第 2 の実施例を説明する。

【0033】第 2 の実施例は、装置動作がマイクロプロセッサ等によるプログラムによる逐次処理による場合には、カウンタ 5 と乱数生成回路 3 の動作は同時並行に行うことができない。このため、カウンタ 5 の値を逐次的に更新するものである。マイクロプロセッサを用いる場合には、起動信号 4 としては、コマンドにより契機信号が入力されるものとする。

【0034】図 3 は、本発明の第 2 の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【0035】カウンタ 5 は、外部からの起動信号 4 が入力されない限り、内部クロック 6 に同期してカウントアップ  $C \leftarrow G(C)$  を繰り返す (ステップ 201)。外部からの起動信号 4 が入力された場合に限り (ステップ 202)、乱数関数回路 3 は、レジスタ 2 の値 R とその時点のカウント 5 の値 C から乱数関数 F (R, C) を生成し、この乱数関数によりレジスタ 2 の値 R を更新する ( $R \leftarrow F(R, C)$ )。

【0036】本実施例では、起動信号 4 が内部クロック 6 と独立に発生することが重要であり、前述の第 1 の実施例と同じ探索空間に広げる効果がある。

【0037】なお、従来の RSA 暗号により相手認証を行う場合の有効な手段として説明した場合と同様に、疑

似乱数関数 F は、第 2 パラメータ C の他に第 3 パラメータ K を入力して導入し、 $R \leftarrow F(R, C, K)$  とすることもできる。

【0038】上記のように、本実施例によれば、内部クロック 6 に基づいて繰り返し動作するカウンタ 5 と、クロックとは非同期な外部からの起動信号による手段により仮に以下の条件が与えられても、

(1) 装置が全く同じ構造:

(2) 初期化され、同じ状態になる:

(3) 装置使用の技術開示:

カウンタ 5 の取り得る場合の数 T と使用前の乱数更新回数 L により探索空間を T × L 倍に広げることができ、十分な対策となる。

【0039】また、従来は、ある時点における乱数 R を知ることにより、その後の乱数の探索空間を狭めることが可能であったが、上記に実施例によれば、レジスタ 2 の乱数の更新を適当に行うことで、探索空間を T × L 倍に広げることができる。

【0040】

【発明の効果】上述のように本発明によれば、装置が全く同じ構造、初期化され同じ状態になる、装置使用の技術開示がなされているような条件下でも、探索空間を広げることにより、乱数の秘匿性を確保でき、鍵配送や、相手認証等が安全に実行できる。

【図面の簡単な説明】

【図 1】本発明の一実施例の疑似乱数生成装置の構成図である。

【図 2】本発明の第 1 の実施例の疑似乱数生成装置の動作を占めるフローチャートである。

【図 3】本発明の第 2 の実施例の疑似乱数生成装置の動作を示すフローチャートである。

【図 4】従来の疑似乱数生成装置のブロック図である。

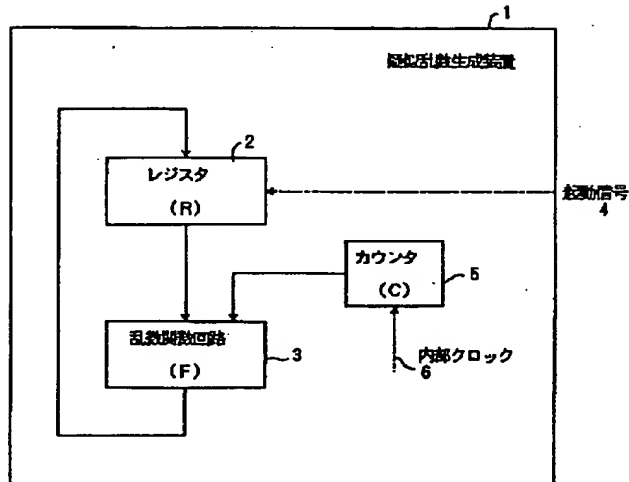
【図 5】従来の疑似乱数生成装置の動作を示すフローチャートである。

【符号の説明】

- 1 疑似乱数生成装置
- 2 レジスタ
- 3 乱数関数回路
- 4 起動信号
- 5 カウンタ
- 6 内部クロック

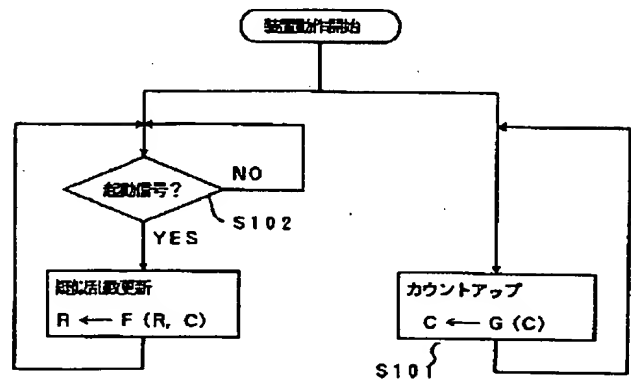
【図 1】

本発明の一実施例の疑似乱数生成装置の構成図



【図 2】

本発明の第 1 の実施例の疑似乱数生成装置の動作を示すフローチャート

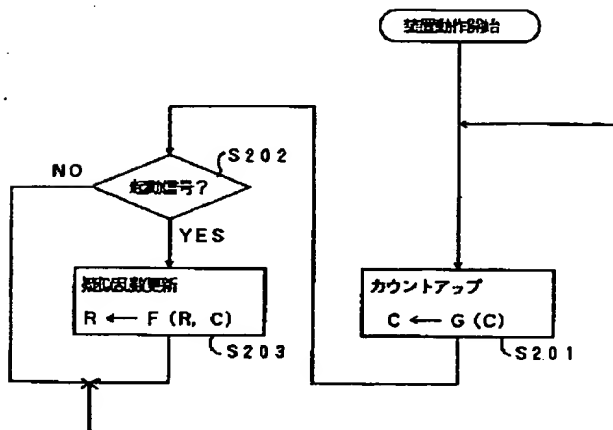


【図 4】

従来の疑似乱数生成装置のブロック図

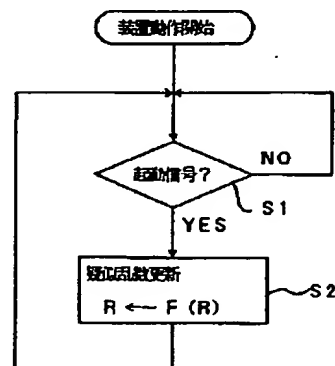
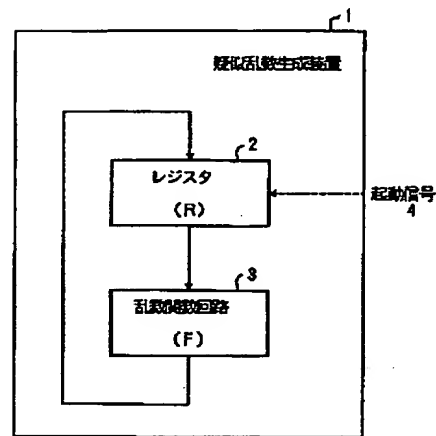
【図 3】

本発明の第 2 の実施例の疑似乱数生成装置の動作を示すフローチャート



【図 5】

従来の疑似乱数生成装置の動作を示すフローチャート



フロントページの続き

(51) Int. Cl.<sup>6</sup>

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/10

9/12